ZIMPERIUM®

L'état de la sécurité des applications financières mobiles

Contenus

Introduction 2

Conclusions principales 3

État de la sécurité des applications financières 4

Risques liés aux appareils mobiles Finance app threat 4
Contexte des menaces qui pèsent sur les applications financières 5
Risques liés à la sécurité des applications financières 6

quel point les applications financières d'au ourd'hui sont-elles sécurisées 7
Ce que nous avons testé 7
Principales menaces réelles détectées 8
Conclusions détaillées 9
Sécurité des applications par SE 9
Sécurité des applications par pays/région 11
Sécurité des applications par type d'application financière 12
Problèmes relatifs à la cryptographie 13

Renforcer la sécurité des applications 14

Annexe 16

Sources 17

Introduction

Les changements drastiques de l'année dernière ont poussé les organisations et les consommateurs à changer la manière dont ils réalisent toutes leurs opérations financières. Les interactions hors-ligne étant entravées par la pandémie de la COVID- , l'utilisation des applications mobiles financières et des autres canaux numériques a explosé à travers le monde.

Selon Fidelity National Information Services, les nouvelles inscriptions aux services bancaires mobiles ont bondi de 200 % rien qu'en avril 2020.[1] Au cours de l'année écoulée, le temps passé sur les applications financières a augmenté de 45 %,[2] l'activité dans les applications d'investissement a augmenté de 88 %[3] et les transactions au point de vente des portefeuilles mobiles ont augmenté de 19,5 %, ces hausses ont été facilités par les limites plus élevées pour les paiements sans contact.[4]

Tandis que les organisations se démenaient pour répondre à la hausse de la demande, les cybercriminels en ont profité. En juin, le FBI a émis une alerte relative à la hausse des attaques contre les applications financières mobiles, notamment les chevaux de Troie bancaires et les applications bancaires fausses/clonées.

L'évolution rapide du contexte des menaces oblige les institutions financières à donner la priorité à la sécurité de leurs applications mobiles. Les entreprises de technologie financière y parviennent jusqu'à un certain point. Une enquête de Verizon a révélé que 92 % des sociétés de services financiers déclarent que les organisations doivent prendre la sécurité mobile plus au sérieux. Pourtant, 43 % d'entre elles ont sciemment sacrifié la sécurité mobile pour respecter un délai ou un objectif de productivité[5] malgré une multitude de réglementations de sécurité - nouvelles ou mises à jour - qui devraient entrer en vigueur en 2021.

Jusqu'à quel point les applications financières mobiles d'aujourd'hui sont-elles bien équipées pour relever ces défis permanents ? Pour comprendre les plus grandes menaces à la sécurité des applications financières dans le monde, Zimperium a examiné un échantillon d'applications mobiles, y compris des applications de paiement sans contact, dans plusieurs zones géographiques. Ce rapport présente les résultats de cette analyse, ainsi que des stratégies pour aider les développeurs des applications financières et les organisations à limiter les risques et à atténuer les vulnérabilités.

Conclusions principales

L'évaluation a révélé de sérieuses failles de sécurité dans les applications financières mobiles et ce, dans tous les domaines et dans toutes les régions.

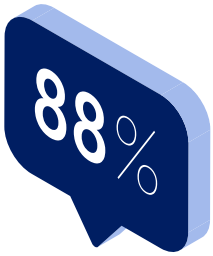
1

des applications ont au moins une vulnérabilité des applications critique ou très grave

2

des applications financières ont des fuites de données

3



échouent aux tests cryptographiques

4

des applications de paiement sont vulnérables à l'extraction de clés de chiffrement

5

Les applications financières britanniques contiennent le moins de vulnérabilités critiques

6

Les applications bancaires contiennent plus de vulnérabilités que tout autre type d'application financière

7

Près des 3/4 des menaces très graves auraient pu être atténuées à l'aide d'une protection intégrée à l'application

État de la sécurité des applications financières

La pandémie mondiale a grandement accéléré le rythme de l'adoption des applications financières mobiles. Les paiements mobiles, en particulier, ont été propulsés à des années d'avance sur les prévisions.[6]

Cependant, dans le cadre d'une stratégie axée sur le mobile, de nombreuses organisations financières relèguent la sécurité des applications au dernier tour. Au mieux, cela peut faire dérailler le progrès. Au pire, cela laisse des failles de sécurité qui entraînent de graves conséquences. Les cybercriminels exploitent des applications vulnérables pour voler les identifiants et les renseignements personnels des utilisateurs, pour accéder aux actifs financiers des clients ou pour même insérer des portes dérobées dans les systèmes d'entreprise d'une organisation.

Cela expose les organisations non seulement au risque de vol de fonds et d'amendes réglementaires, mais peut également avoir un impact sur l'acquisition et la fidélisation des clients. Tandis que la pandémie a poussé les clients vers les canaux numériques, 41 % des utilisateurs de services bancaires mobiles expriment toujours de grandes préoccupations concernant l'utilisation illégale de leurs renseignements personnels et des informations de leur compte et 38 % s'inquiètent au sujet des transferts de fonds frauduleux. Les failles de sécurité des applications pourraient pousser ces clients vers d'autres fournisseurs ou vers l'abandon complet de ces canaux une fois que la sécurité sanitaire n'aura plus d-influence sur leur comportement.

Risques liés aux appareils mobiles

De nombreux appareils mobiles contiennent des mécanismes de sécurité matérielle, tels que des processeurs cryptographiques intégrés ou des environnements d'exécution de confiance (TEE).¬ Toutefois, ils ne sont pas toujours disponibles et le manque de normalisation entre les TEE fait que les niveaux de sécurité varient d'un appareil à l'autre. De plus, le soutien matériel n'est pas synonyme d'impénétrabilité. Les attaquants peuvent utiliser l'analyse de puissance différentielle (DPA) ou d'autres méthodes d'attaque par canal auxiliaire pour extraire les clés.

De plus, de graves failles de sécurité des SE mobiles sont continuellement révélés. Rien qu'au premier trimestre de 2021, Google a corrigé 121 vulnérabilités critiques et très graves dans son système d'exploitation Android.[7] Au cours de la même période, Apple a résolu 54 problèmes de sécurité dans iOS.[8] Et en juillet 2020, un groupe de pirates a découvert une vulnérabilité permanente dans la puce Apple Secure Enclave qui pourrait mettre en danger les clés de chiffrement.[9]

Les appareils jailbreakés ou rootés constituent une autre menace sérieuse. Les fournisseurs d'applications financières n'ont aucun contrôle sur l'appareil sur lequel leur application est installée et une fois que celui-ci est jailbreaké ou rooté, les contrôles de sécurité du système d'exploitation sont compromis et des éléments tels que les clés de chiffrement peuvent être lues en clair si aucun modèle Zéro confiance n'a été prévu et mis en œuvre dans le cadre de votre posture de sécurité.

Contexte des menaces qui pèsent sur les applications financières

Les logiciels malveillants qui ciblent les applications financières mobiles demeurent l'une des cybermenaces à la croissance et à l'évolution les plus rapides. En 2020, 156 710 nouveaux chevaux de Troie bancaires mobiles ont été détectés, soit plus du double par rapport à l'année précédente.[10]

Beaucoup d'entre eux ont joué sur les craintes associées à la pandémie. De nombreuses fausses applications de recherche de contacts COVID ont livré des chevaux de Troie bancaires SpyNote et Anubis. Une fois installé, Anubis injecte une superposition qui se place au-dessus de l'application bancaire et capture les identifiants bancaires, le PIN et les autres renseignements personnels précieux.[11] Les attaques sur le thème de la cryptomonnaie étaient également populaires, certaines ciblaient les portefeuilles crypto, d'autres installaient des logiciels malveillants bancaires généraux, tels qu'un convertisseur de cryptomonnaie - sanctionné par Google Play Store - qui diffusait le cheval de Troie Cerberus.[12]

Les menaces qui pèsent sur la finance mobile continuent de devenir de plus en plus sophistiquées, en adoptant de nouvelles techniques pour voler des données tout en évitant la détection par les outils de sécurité. Par exemple, le nouveau cheval de Troie bancaire Ghimob identifie et surveille les applications financières installées sur un appareil, capture les informations de l'appareil et du compte en exploitant les fonctionnalités d'accessibilité et, lorsqu'il est prêt, effectue la transaction frauduleuse en arrière-plan tandis que l'utilisateur regarde un écran de superposition. En piratant l'appareil, il échappe aux mesures d'identification de la machine et de sécurité anti-fraude mises en place par les institutions financières.[13]

Les émulateurs qui usurpent les appareils pour accéder aux applications constituent une autre menace. À la fin de 2020, un gang de cybercriminels a volé des millions de dollars à des institutions financières américaines et européennes en utilisant des données volées et en émulant les appareils mobiles des titulaires de compte pour effectuer des transactions frauduleuses. [14]

Les applications bancaires, fausses ou clonées, sont un autre vecteur d'attaque qui demeure actif. Les applications authentiques sont soumises à une ingénierie inverse pour en obtenir le code source qui est ensuite falsifié pour créer une version malveillante qui sera reconditionnée et diffusée via des sites web contrefaits ou publiée dans des magasins d'applications. Une fois installées, leur page d'accueil est un formulaire qui sert à capturer les identifiants de connexion ou les informations de la carte bancaire pour voler des fonds.

Risques liés à la sécurité des applications financières

Les organisations financières peuvent ne pas être en mesure de contrôler les environnements dans lesquels leurs applications s'exécutent ou les menaces que les cybercriminels génèrent, mais elles sont responsables du code de leur application. L'OWASP (Open Web Application Security Project) tient à jour une liste des dix principaux types de vulnérabilités d'applications mobiles qui posent les plus grands risques de sécurité pour les organisations et les utilisateurs.[15]

Les pratiques de codage et les applications non sécurisées peuvent entraîner des fuites de données, des communications non sécurisées, des problèmes d'authentification et d'autorisation, une cryptographie faible, un risque de falsification du code et une vulnérabilité à l'ingénierie inverse. Cela crée des brèches qui permettent aux attaquants de voler des informations personnelles et financières, d'exfiltrer des clés de chiffrement, d'injecter des logiciels malveillants dans l'application et de pirater les processus de celle-ci. Les vulnérabilités testées dans notre analyse relèvent toutes d'une ou plusieurs des catégories de risque de l'OWASP.

Les 10 principaux risques de l'OWASP pour les appareils mobiles

M1	**Utilisation inappropriée de la plateforme**
M2	**Stockage de données non sécurisé**
M3	**Communications non sécurisées**
M4	**Authentification non sécurisée**
M5	**Faible cryptographie**
M6	**Autorisation non sécurisée**
M7	**Qualité du code client**
M8	**Falsification du code**
M9	**Ingénierie inverse**
M10	**Fonctionnalité extrinsèque**

À quel point les applications financières d'aujourd'hui sont-elles sécurisées ?

Compte tenu de la pandémie qui a accéléré l'adoption des applications financières mobiles à l'échelle mondiale et l'augmentation concomitante des attaques contre celles-ci, la sécurité de ces applications devrait être la priorité absolue pour les organisations.

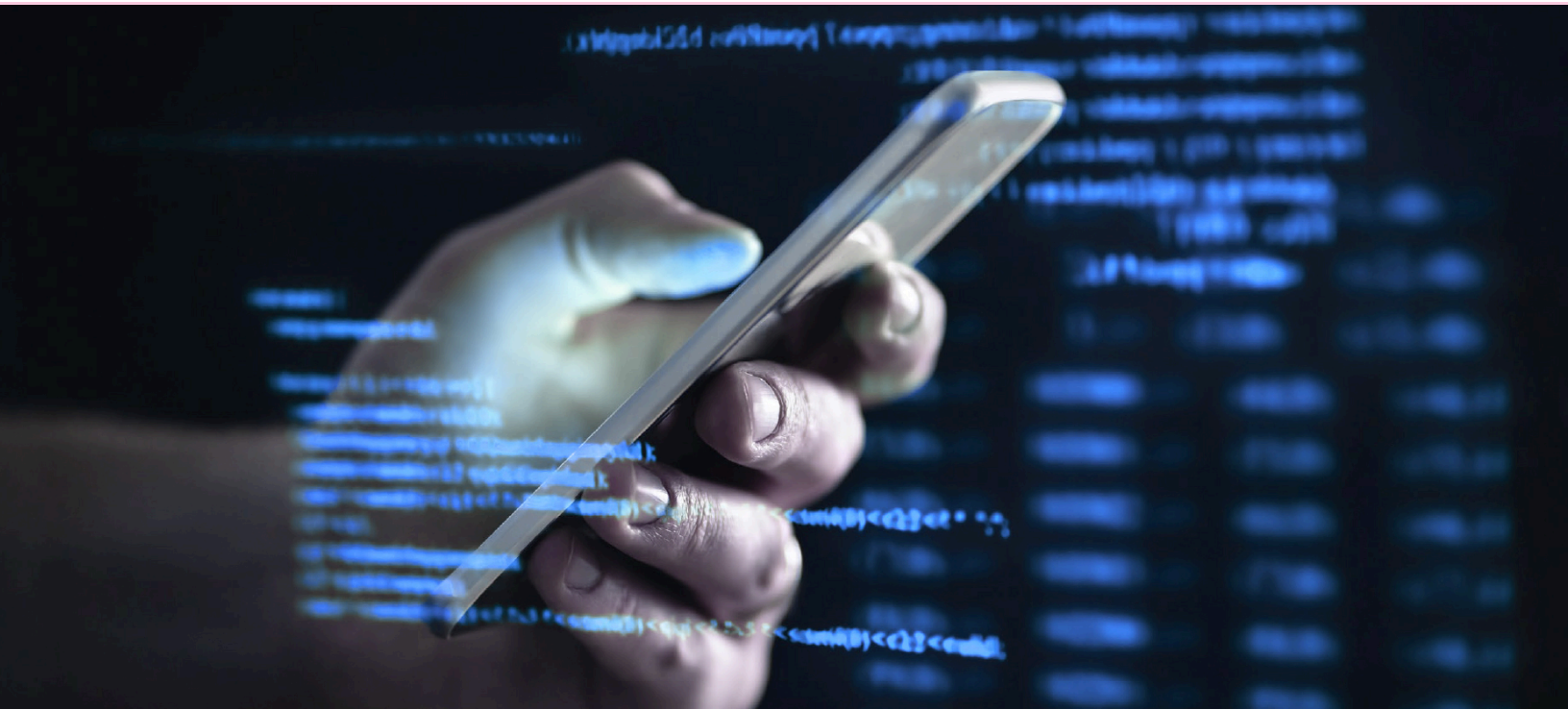
Cette étude a évalué les applications dans 5 pays ou régions (les États-Unis, l'Inde, le Royaume-Uni, l'Union européenne et l'Asie du Sud-Est) pour déterminer le niveau de sécurité des applications financières dans le monde et leur résilience aux cybermenaces.

Ce qui a été testé

Des évaluations de sécurité ont été menées sur 160 applications de services financiers mobiles accessibles au public dans quatre catégories principales : la banque, le paiement mobile, l'investissement / le trading et le prêt. Toutes les applications ont été téléchargées directement depuis leurs magasins respectifs (App Store® d'Apple Inc. et Google Play™) et ont été sélectionnées en fonction du nombre de téléchargements et de la taille de l'organisation.

Les applications ont été analysées à l'aide de tests statiques de sécurité des applications (SAST) et de tests dynamiques de sécurité des applications (DAST) et ce, conformément aux directives de l'OWASP.

Les menaces ont été classées comme « Faible », « Moyenne », « Élevée » et « Critique » selon le système de notation des vulnérabilités (CVSS). Voir l'annexe pour les détails de la classification et la liste complète des vulnérabilités testées



Principales menaces réelles détectées

Même si presque tous les types de vulnérabilités ont été détectés dans plusieurs applications, certaines menaces se sont démarquées en termes de gravité, de prévalence ou des deux.

Vulnérabilité	Pourquoi est-elle important	Catégorie OWASP	Violation potentielle de la norme PCI-DSS	Pourcentage des applications testées affectées
Stockage d'informations non cryptées dans les préférences partagées	Les préférences partagées sont un ensemble d'API dans Android qui permettent aux applications de stocker et de récupérer des données depuis l'appareil. Les informations sensibles non cryptées ne doivent jamais être stockées dans les préférences partagées, car les données sont facilement lisibles et modifiables par les attaquants et les applications malveillantes.	M2 : Stockage de données non sécurisé	Les sections 3.2, 3.3, 3.4 concernant la protection des données stockées des titulaires de carte	73 % des applications Android
Clés cryptographiques dérivées faibles	L'API de sécurité Java Android prédominante utilise par défaut le mode de chiffrement par bloc ECB pour le chiffrement AES, qui est considéré comme étant moins sécurisé que les autres méthodes et ce, car il génère le même texte chiffré pour les blocs identiques de texte brut. Les développeurs qui s'appuient sur le processus de cryptage par défaut fourni par le système d'exploitation s'exposent au risque de vol d'informations et de code.	M5: Faible cryptographie	Les sections 3.5, 3.6 concernant la protection des données stockées des titulaires de carte	61 % des applications Android
Validation SSL CA et épinglage de certificat désactivés	L'épinglage associe un hôte à son certificat X.509 ou à sa clé publique prévus. La méthode d'épinglage la plus sécurisée ajoute le certificat ou la clé publique à l'application pendant la phase de développement. Si l'épinglage de certificat est mal implémenté, les attaquants peuvent utiliser de faux identifiants pour accéder au trafic entre l'application et le serveur web et voler des données confidentielles.	M3: Communications non sécurisées	La section 4.1 qui exige un cryptage renforcé pour l'authentification et la transmission des données du titulaire de la carte sur les réseaux publics	60 % des applications Android
Mauvaise configuration de l'App Transport Security (ATS)	L'ATS est une fonction de sécurité réseau iOS qui garantit que les connexions réseau utilisent les protocoles et les chiffrements les plus sécurisés. Lorsqu'elle est mal utilisée, les données peuvent être interceptées et exploitées.	M3: Communications non sécurisées	La section 4.1 qui exige un cryptage renforcé pour l'authentification et la transmission des données du titulaire de la carte sur les réseaux publics	65 % des applications iOS
Stockage de données non sécurisé dans les applications iOS	Il s'agit en fait d'une combinaison de plusieurs vulnérabilités. Nous avons trouvé plusieurs instances d'applications iOS qui stockent des données sensibles dans des endroits qui n'ont aucune prise en charge intégrée du chiffrement. Cela signifie que les informations sensibles sont stockées sous forme de texte clair, à moins que des mécanismes de chiffrement personnalisés, tels que la cryptographie en boîte blanche, ne soient utilisés.¬¬ Si le périphérique local est compromis, les données stockées le sont également.	M2 : Stockage de données non sécurisé	Les sections 3.2, 3.3, 3.4 concernant la protection des données stockées des titulaires de carte	Applications iOS stockant des informations sensibles dans : NSUserDefaults : 61 % Listes de propriétés : 55 % Bases de données SQLite3 : 46 %

Conclusions détaillées

Chaque application testée présentait au moins un problème de sécurité de base. En approfondissant l'analyse, 88 % avaient des problèmes cryptographiques, 81 % peuvent avoir des fuites de données et 77 % contenaient des failles qui présentent des risques de haut niveau pour les organisations financières et leurs clients. Ces résultats suggèrent que l'attention accrue portée aux risques de cybersécurité et le resserrement des réglementations ne se sont pas traduits par des applications financières mobiles sécurisées. Les applications des quatre catégories financières révèlent des pratiques de codage non sécurisées répandues, ainsi qu'un manque général des contrôles de sécurité et des protections technologiques intégrées aux applications, telles que le blindage des applications, l'autoprotection des applications d'exécution (RASP) et la protection par clé cryptographique en boîte blanche.

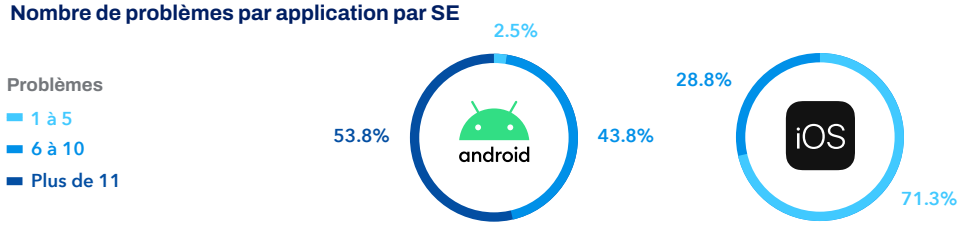
Nous avons trouvé des différences dans le niveau de sécurité des types d'applications ainsi que des disparités importantes entre les régions. Toutefois, nous devons être prudents avant de tirer des conclusions définitives concernant les caractéristiques régionales, car il n'y avait pas une parité à 100 % entre les types des applications testées. Par exemple, les échantillons de test de l'UE comprenaient plus d'applications de paiement que les autres régions, tandis que l'échantillon de l'Inde contenait plus d'applications entrant dans la catégorie du trading. Néanmoins, ces écarts ne peuvent expliquer les différences régionales assez spectaculaires.

Sécurité des applications par SE

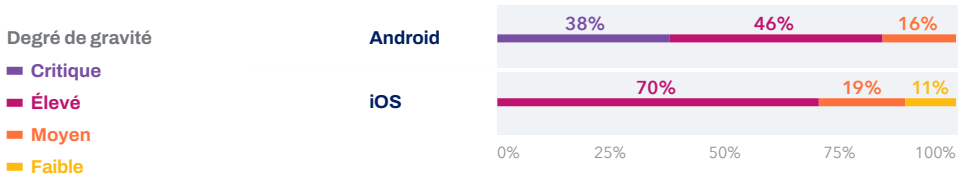
De nombreuses organisations supposent qu'iOS est une plateforme intrinsèquement plus sécurisée qu'Android, mais la plus grande popularité d'Android parmi les utilisateurs et les attaquants rend les comparaisons injustes. L'élément incontestable est que les deux se classent parmi les dix systèmes d'exploitation les plus vulnérables en matière de nombre total de vulnérabilités distinctes. Que ce soit sur l'une ou l'autre plateforme, les développeurs ne peuvent pas compter sur les protections du système d'exploitation pour sécuriser leurs applications, d'autant plus que le jailbreaking et le rooting restent répandus.[16]

Lors de nos tests, les applications Android ont présenté beaucoup plus de problèmes que les applications iOS. Par application, presque toutes les applications financières Android (97,5 %) présentaient plus de cinq failles de sécurité, contre environ 30 % des applications iOS. Cependant, lorsqu'on examine le degré de gravité, l'écart se réduit. Environ 84 % des applications financières Android présentaient au moins une vulnérabilité critique ou très grave, contre 70 % des applications iOS.

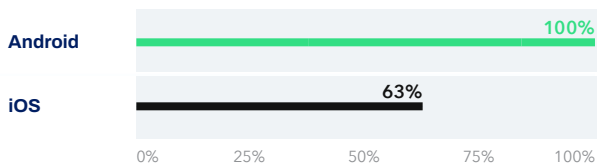
Nombre de problèmes par application par SE



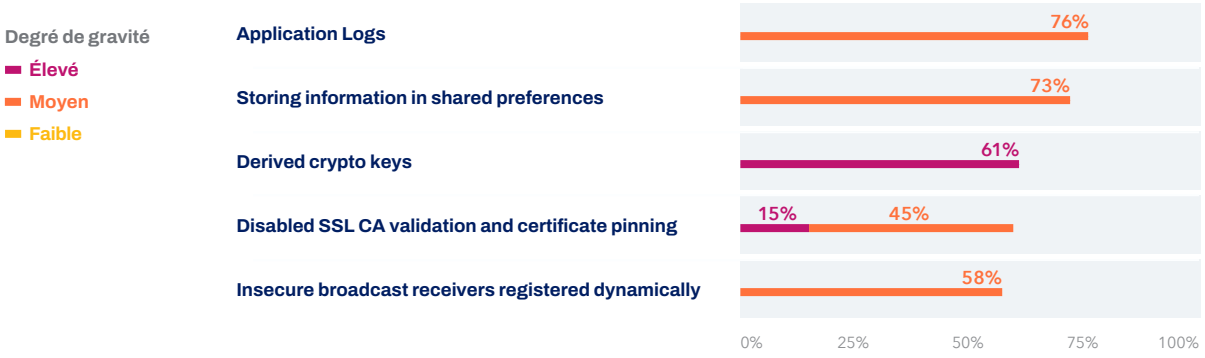
Répartition des vulnérabilités par SE



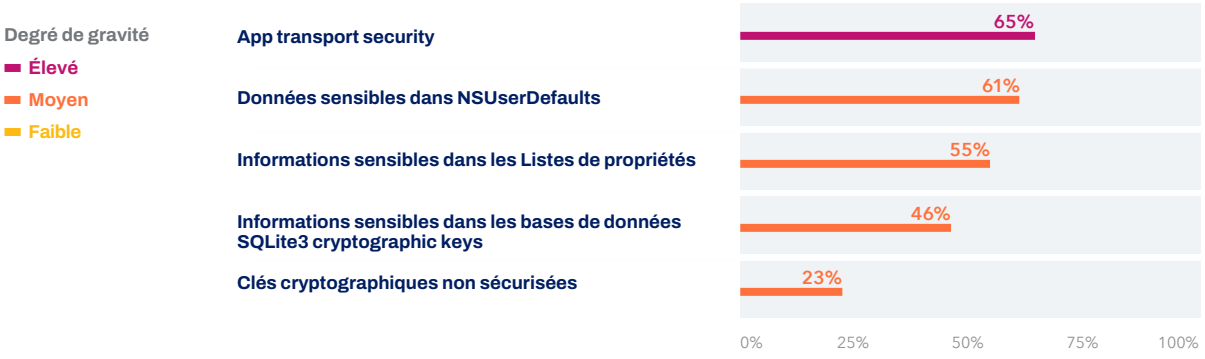
Applications présentant une vulnérabilité de fuite de données par SE



Top five significant vulnerabilities found: Android apps



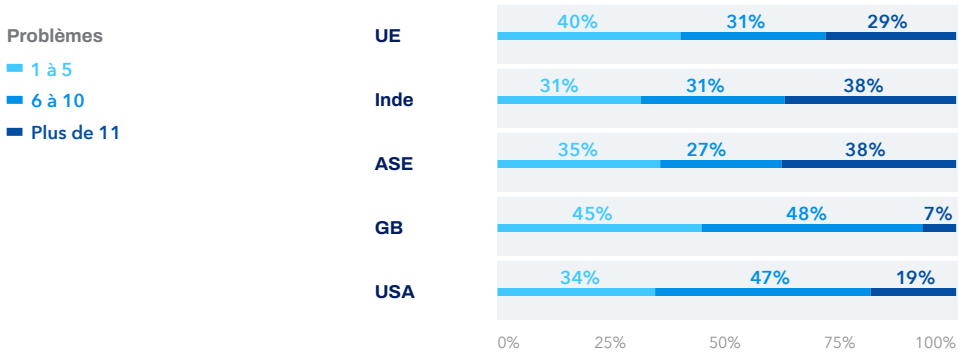
Les cinq principales vulnérabilités trouvées : applications iOS



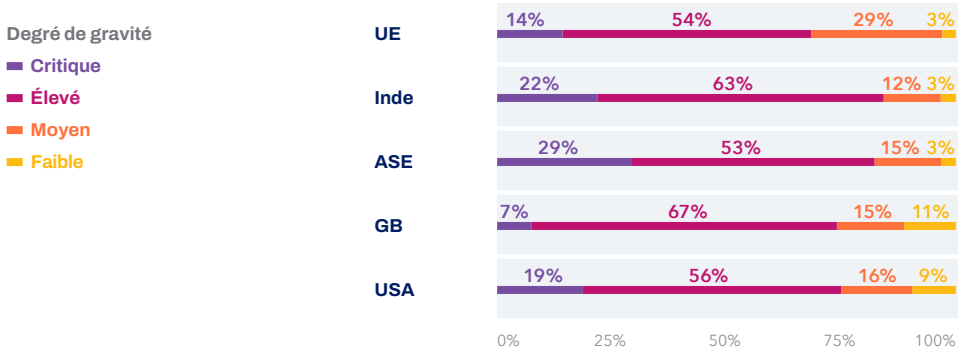
Sécurité des applications par pays/région

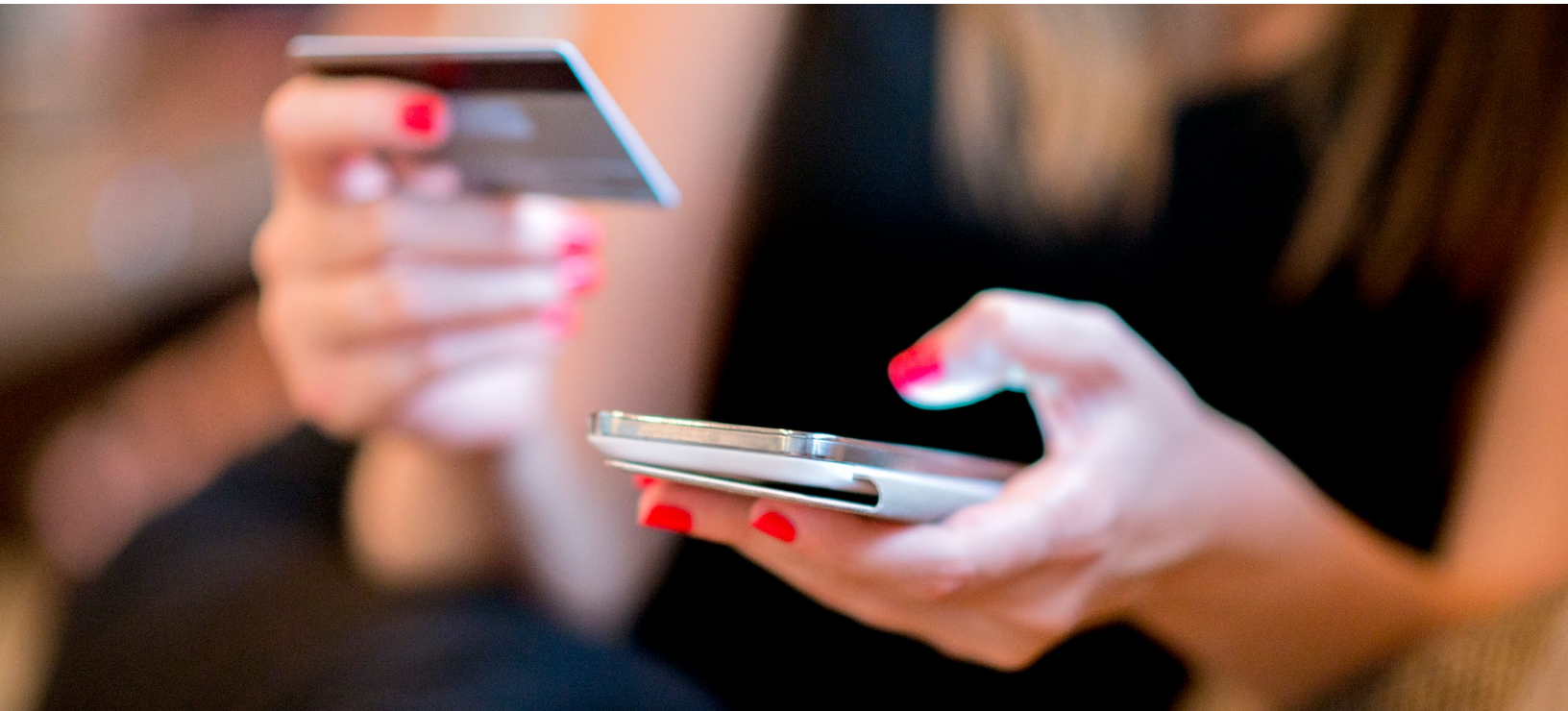
Concernant les niveaux de sécurité des applications, nous avons trouvé des écarts importants entre les zones géographiques. GB Les applications financières du Royaume-Uni avaient beaucoup moins de problèmes de sécurité que les applications des autres régions : seulement 7 % présentaient plus de 10 vulnérabilités, contre 38 % des applications financières en Inde et en Asie du Sud-Est, 29 % en UE et 19 % aux États-Unis. Les applications du Royaume-Uni contenaient également le plus petit nombre de vulnérabilités critiques par rapport aux autres régions. Les applications d'Asie du Sud-Est et d'Inde ont affiché les performances les plus faibles en termes de sécurité. Les résultats suggèrent que les réglementations strictes en matière de sécurité des services financiers et de confidentialité des données au Royaume-Uni et dans l'UE ont un fort impact sur la sécurité des applications financières. Au-delà des exigences elles-mêmes, qui fournissent en règle générale une base de référence minimale, ces réglementations incitent les développeurs des applications à comprendre les considérations de sécurité et à prendre la défense des applications plus au sérieux.

Nombre de problèmes détectés par pays/région



Breakdown of vulnerability severity by country/region

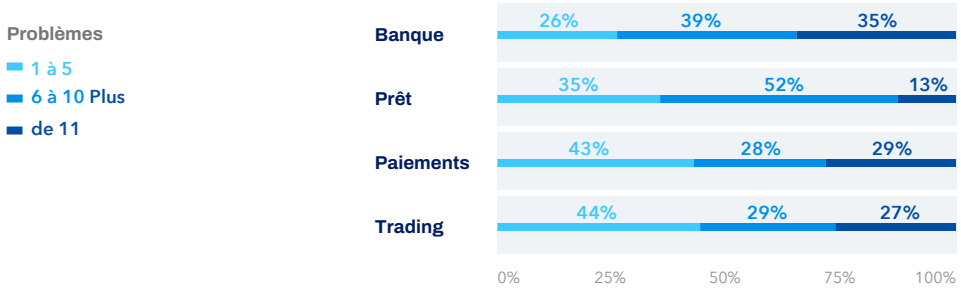




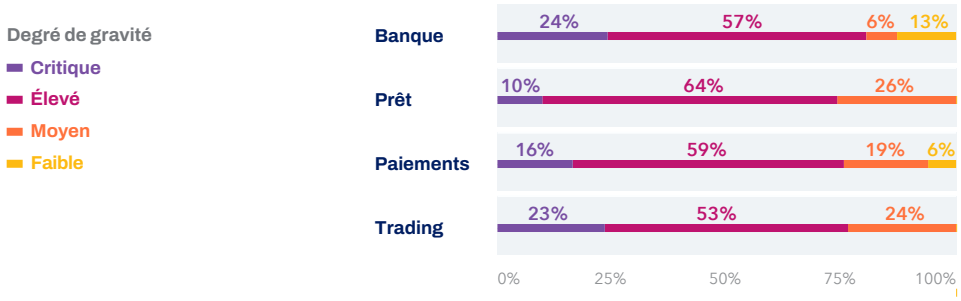
Sécurité des applications par type d'application financière

En examinant les différentes catégories des applications financières mobiles, nous avons découvert des résultats surprenants. Les applications bancaires se sont avérées nettement plus vulnérables, tant en termes de nombre total de problèmes que de gravité, 35 % d'entre elles présentaient plus de 10 vulnérabilités et 81 % au moins un problème critique ou très grave. Les applications de paiement ne s'en sortent que légèrement mieux, avec 29 % et 75 %, respectivement. Les applications de prêt ont occupé la meilleure place, peut-être que c'est dû à leurs fonctionnalités plus limitées.

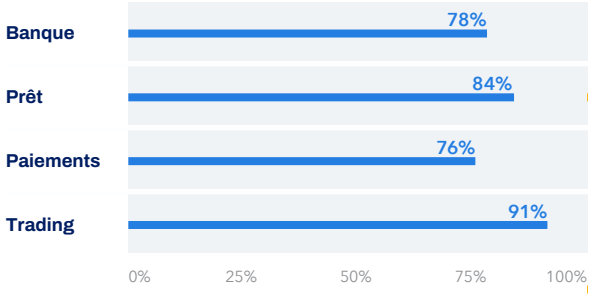
Nombre de problèmes détectés par type d'application



Répartition de la gravité des vulnérabilités par type d'application



Breakdown of data leak vulnerability by app type

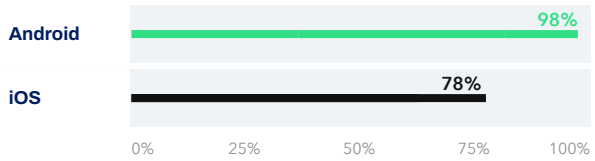


Problèmes relatifs à la cryptographie

Nous répartissons les problèmes relatifs à la cryptographie dans une catégorie distincte, car cela continue d'être un sujet de préoccupation pour les applications financières dans tous les domaines et dans toutes les régions. 88 % des applications testées présentaient au moins un problème de cryptographie important (gravité moyenne ou élevée), notamment des clés de chiffrement exposées, une mauvaise mise en œuvre des algorithmes cryptographiques, une taille de clé insuffisante et des défaillances dans le chiffrement sécurisé des communications de données sensibles.

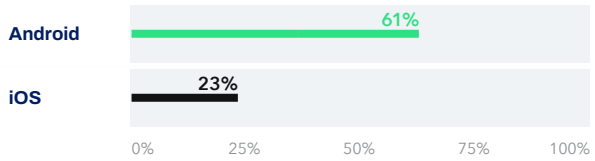
Au sein de cette catégorie de vulnérabilités, la prédisposition à l'extraction des clés cryptographiques mérite une attention particulière, car elle expose les organisations à des risques de fraude financière et ainsi qu'à une responsabilité légale. L'analyse a révélé que 61 % des applications Android et 23 % des applications iOS sont vulnérables à l'extraction des clés de chiffrement. Lors de la répartition des chiffres par zone géographique et par type d'application, les tendances que nous avons constatées dans les sections précédentes se maintiennent. Les applications britanniques s'en sont bien mieux tirées que leurs homologues dans les autres régions, tandis que les applications bancaires et de paiement se sont avérées les plus faibles parmi toutes les catégories d'applications en termes de sécurité des clés de chiffrement.

Nombre d'applications présentant un problème de cryptographie grave*

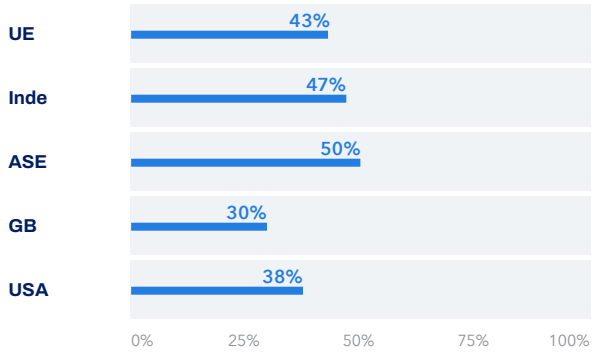


* grave signifie une vulnérabilité de gravité moyenne ou élevée

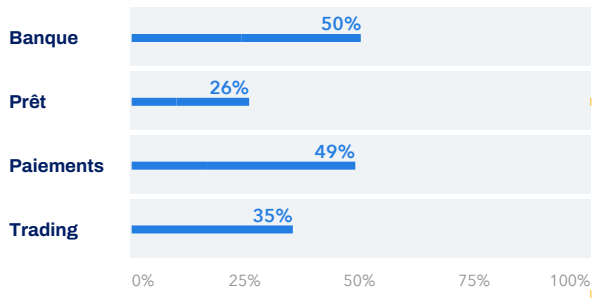
Nombre d'applications vulnérables à l'extraction de clés de chiffrement



Répartition de la vulnérabilité à l'extraction de clé de chiffrement par pays/région



Répartition de la vulnérabilité à l'extraction de clé de chiffrement par type d'application



Renforcer la sécurité des applications financières

Cette étude a révélé un décalage entre le niveau de préoccupation, concernant les menaces mobiles, exprimé par les organisations de services financiers (85 % ont évalué le risque comme modéré à important) et le niveau de sécurité des applications qu'elles et leurs clients utilisent.[17]

L'essor de l'adoption des applications financières mobiles, la portée croissante des services financiers mobiles et l'évolution du contexte des menaces indiquent tous que les développeurs doivent donner la priorité à la réduction du nombre de vulnérabilités dans leurs applications et ce, quel que soit le secteur ou le pays dans lequel ils opèrent.

Construire une base solide

Les développeurs de logiciels mobiles de services financiers devraient, au moins, suivre les pratiques de base en matière de conception d'applications sécurisées. La norme OWASP de vérification de la sécurité des applications mobiles est une excellente ressource. Effectuer des tests réguliers et suivre un framework DevSecOps afin que la sécurité fasse partie du cycle de vie du développement.

Veillez à rester au courant des derniers changements réglementaires et des exigences de conformité en matière de sécurité, telles que le RGPD et le PCI-DSS. Une bonne évaluation des risques exige que vous soyez conscient de votre état de sécurité et de celui de votre utilisateur.

Améliorations et atténuations spécifiques recommandées

- Ne stockez pas de données sensibles dans des emplacements non sécurisés où elles peuvent être facilement extraites et exploitées. Ces informations doivent être protégées à l'aide de technologies de chiffrement sécurisé, telles que la cryptographie en boîte blanche ou en utilisant des techniques renforcées de camouflage des données.
- La grande majorité des applications de services financiers (88 %) ont un chiffrement mal géré et/ou faible qui les expose au risque de vol de données. Des technologies de protection des clés, comme la cryptographie en boîte blanche, doivent être utilisées pour sécuriser le processus de chiffrement.
- Presque toutes les applications de services financiers testées ne disposaient pas de protections pour détecter et arrêter les analyses et l'ingénierie inverse menées par les pirates. Les protections contre la falsification et l'exécution sont essentielles dans ce domaine.

Renforcer la sécurité avec la protection intégrée à l'application

La croissance rapide des applications financières et leur valeur en tant que cible lucrative signifie que les menaces sont devenues plus fréquentes, plus complexes et plus difficiles à empêcher à l'aide des mesures de sécurité de base.

Il est impossible d'éliminer toutes les vulnérabilités des applications. Les technologies de protection intégrées à l'application ajoutent des mécanismes de sécurité à la vôtre afin qu'elle devienne beaucoup plus difficile à pénétrer, à modifier ou à soumettre à l'ingénierie inverse. Cela implique un certain nombre de techniques de protection, notamment le camouflage avancé du code, l'anti-débogage, la détection du jailbreaking iOS et du rooting Android, la protection de l'intégrité, ainsi que la détection et la réponse aux falsifications. Les outils les plus robustes protègent les applications contre les menaces statiques et dynamiques ainsi que contre les attaques par canaux auxiliaires, telles que l'analyse différentielle des défauts et l'analyse différentielle de puissance.

Protéger les clés cryptographiques

Les cryptages les plus robustes ne peuvent pas protéger les données ou les communications si les clés de chiffrements sont compromises. Des attaquants talentueux les retirent du code ou de la mémoire, car elles sont utilisées dans des opérations cryptographiques. Même si les magasins de clés fournis par les SE offrent une certaine protection, leur sécurité ne peut pas être garantie pour tous les appareils sur lesquels votre application s'exécute et, lorsqu'ils sont rootés, ils n'offrent aucune protection. Utilisez la cryptographie en boîte blanche pour intégrer une protection de clé directement dans vos applications

Zimperium peut vous aider

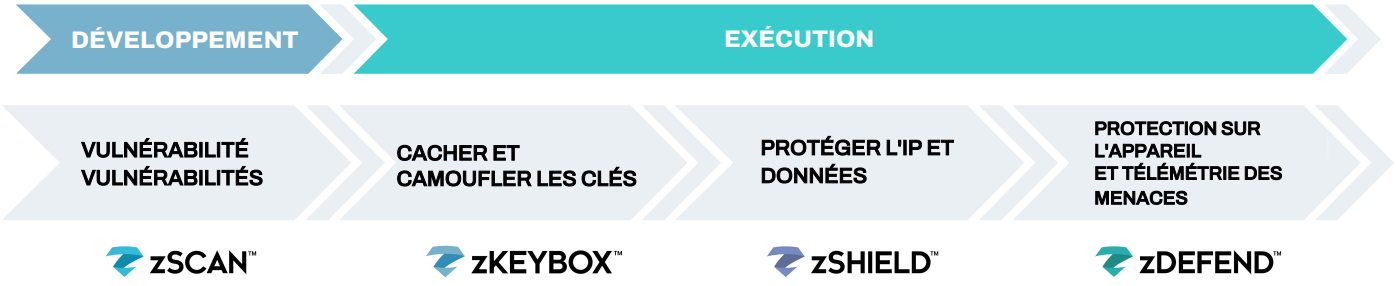
Zimperium fournit de puissantes solutions de protection intégrées aux applications et de cryptographie en boîte blanche qui protègent les applications contenant des informations sensibles, déjouent les attaques et vous aident à vous conformer aux réglementations en vigueur dans l'industrie. Notre équipe jouit d'une grande expérience dans le domaine de la sécurité des applications financières.

Zimperium zScan
aide les développeurs des applications mobiles à identifier les risques de réputation et financiers en détectant automatiquement les risques de confidentialité, de sécurité et de conformité dans le processus de développement et ce, avant la publication des applications.

Zimperium zShield
injecte des capacités d'autodéfense dans les applications, leur permettant ainsi de s'exécuter en toute sécurité dans des environnements Zéro confiance. Il utilise plusieurs méthodes, notamment le camouflage du code et la détection des intrusions en temps réel pour empêcher la falsification, l'ingénierie inverse et les autres techniques utilisées par les cybercriminels pour découvrir les vulnérabilités et accéder aux informations et ressources sensibles contenues dans les applications de services financiers.

Zimperium zKeyBox
utilise une cryptographie en boîte blanche à la pointe de la technologie pour garder les clés cryptographiques secrètes bien cachées dans le code de l'application et ce, même pendant l'exécution. Simple à intégrer et à utiliser, il fournit un ensemble complet de méthodes avancées pour fonctionner avec les algorithmes cryptographiques les plus populaires sur n'importe quelle plateforme.

Zimperium zDefend
est un SDK qui permet aux applications mobiles de déterminer immédiatement quand l'appareil d'un utilisateur est compromis, si des attaques réseau sont en cours et même si des applications malveillantes sont installées. Les développeurs d'applications peuvent configurer des actions correctives appropriées lorsqu'une menace donnée est détectée, réduisant ainsi les fraudes potentielles et protégeant les utilisateurs.



Annexe

Notation des vulnérabilités

Vulnerabilities were rated according to the CVSS[18] which is based on exploitability, scope, impact, and other qualitative metrics.

Échelle de notation qualitative du CVSS

Notation	Score CVSS
Aucune	0,0
Faible	0,1 à 3,9
Moyen	4,0 à 6,9
Élevé	7,0 à 8,9
Critique	9,0 - 10,0

L'implication des dommages collatéraux pour chaque catégorie de menace peut être décomposée comme suit :

Classification des menaces	Impact
Aucune (N)	No potential for loss of assets, revenue or productivity
Faible - Moyenne (L)	Dommages limités aux actifs ou perte mineure de revenus ou de productivité
Moyenne - Élevée (M)	Dommages ou pertes graves
Élevé (H)	Dommages ou perte catastrophiques

Vulnérabilités testées et occurrence

Vulnérabilité	Degré de gravité	Total
Mauvaise configuration de la sécurité réseau : Android	Critique	27
Faibles clés de chiffrement dérivées : Android	Élevé	49
JavaScript CORS activé dans Webview : Android	Élevé	39
Protection insuffisante de la couche de transport : Android	Élevé	30
Vulnérabilité de traversée de fichier du fournisseur de contenu : Android	Élevé	4
Contournement de la liste blanche HTTPS de PhoneGap : Android	Élevé	0
Débogage des applications : Android	Élevé	0
Vulnérabilité de redirection d'URL à distance : Android	Élevé	0
Vulnérabilité de manipulation de la page de démarrage à distance Cordova : Android	Élevé	0
SSLSocketFactory non sécurisé : Android	Élevé	0
Vulnérabilité de redirection d'URL d'erreur PhoneGap : Android	Élevé	0
Vulnérabilité de contournement HTTPS PhoneGap : Android	Élevé	0
Exécution à distance du code de l'interface JavaScript : Android	Élevé	0
Connexion au serveur Redis externe : Android	Élevé	0
Validation SSL CA et épinglage de certificat désactivés : Android	Moyen-Élevé	48
Journaux des applications : Android	Moyen	61
Stockage des informations dans les préférences partagées : Android	Moyen	58
Récepteurs de diffusion non sécurisés enregistrés dynamiquement : Android	Moyen	46
Informations sensibles dans la base de données SQLite : Android	Moyen	44
Gestionnaire de confiance SSL hors service : Android	Moyen	29
MediaProjection : AndroidService permet l'enregistrement de l'audio et de l'activité de l'écran : Android	Moyen	28
Piratage de composants Android via Intent : Android	Moyen	27
HostnameVerifier pour SSL hors service : Android	Moyen	25
Application d'extension de WebViewClient : Android	Moyen	24
Données externes dans les requêtes SQL brutes : Android	Moyen	13
Exploits WebView : Android	Moyen	12
Journalisation de débogage PhoneGap : Android	Moyen	9
HostnameVerifier qui autorise tous les noms d'hôte : Android	Moyen	7
URL de la liste blanche de PhoneGap : Android	Moyen	6
Vulnérabilité de désérialisation d'objets Java : Android	Moyen	1
Algorithmes de hachage non sécurisés : Android	Moyen	0
Envoi de données de carnet d'adresses via une couche de transport non cryptée et non sécurisée : Android	Moyen	0
Injection de fragments Android : Android	Moyen	0
Autorisations inutilisées : Android	Faible	79
Activités exportées non protégées : Android	Faible	58
Récepteurs exportés non protégés : Android	Faible	56
camouflage du bytecode manquant : Android	Faible	41

Vulnérabilité	Degré de gravité	Total
Service exporté non protégé : Android	Faible	31
setPluginState obsolète dans WebView : Android	Faible	24
Sauvegarde d'application Android activée : Android	Faible	12
Injection JavaScript PhoneGap : Android	Faible	9
Fournisseur exporté non protégé : Android	Faible	8
Partage subreptice sur Android : Android	Faible	4
Autorisations personnalisées inappropriée : Android	Faible	0
Activités exportées protégées sans signature : Android	Faible	0
Services exportés protégés sans signature : Android	Faible	0
Fournisseurs exportés protégés sans signature : Android	Faible	0
Récepteurs exportés protégés sans signature : Android	Faible	0
Ne pas autoriser WebView à accéder aux ressources locales sensibles via le schéma de fichiers : Android	Faible	0
Autorisations de fournisseur de contenu inappropriées : Android	Faible	0
Services non protégés : Android	Faible	0
Sécurité des transports d'applications : iOS	Faible	52
Accès libre à la liste blanche de PhoneGap : iOS	Élevé	6
Protection insuffisante de la couche de transport : iOS	Élevé	4
Contournement de la liste blanche de PhoneGap RegEx : iOS	Élevé	2
Clés HMAC courtes : iOS	Élevé	2
Exploits UIWebView : iOS	Élevé	1
Données sensibles dans NSUserDefaults : iOS	Élevé	49
Informations sensibles dans les Listes de propriétés : iOS	Moyen	44
Informations sensibles dans les bases de données SQLite3 : iOS	Moyen	37
Clés cryptographiques non sécurisées : iOS	Moyen	18
Données non sécurisées dans CoreData : iOS	Moyen	10
Journalisation de débogage avec NSLog : iOS	Moyen	6
Données non sécurisées dans RealmDB : iOS	Moyen	1
Implémentation d'iOS SecKeyEncrypt : iOS	Moyen	1
Journalisation de débogage PhoneGa : iOS	Moyen	0
Données non sécurisées dans YapDB : iOS	Moyen	0
Algorithmes de hachage vulnérables : iOS	Moyen	0
Données non sécurisées dans CouchDB : iOS	Moyen	0
Connexions de pairs non sécurisées : iOS	Moyen	0
Vulnérabilité Zipperdown menant à une attaque par exécution de code à distance : iOS	Faible	77
NSURLConnection obsolète : iOS	Faible	11
iOSBinary avec protection ASLR : iOS	Faible	0

À propos de Zimperium

Zimperium, le leader mondial de la sécurité mobile, fournit la seule protection basée sur l'apprentissage machine contre les menaces Android, iOS et Chromebook. Zimperium protège les terminaux mobiles et les applications contre les attaques d'appareils, de réseau, de hameçonnage et d'applications malveillantes. Basée à Dallas, au Texas, Zimperium est soutenue par Warburg Pincus, SoftBank, Samsung, Sierra Ventures et Telstra Ventures.

Sources

1 https://www.cnbc.com/2020/05/27/coronavirus-crisis-mobile-banking-surge-is-a-shift-likely-to-stick.html

2 State of Mobile 2021, App Annie, January 2021

3 The Mobile Finance Report 2020, Adjust and Apptopia, October 2020

4 The 2021 Global Payments Report, Worldpay from FIS, March 2021

5 Verizon Mobile Security Index 2020 Report, Verizon, February 2020

6 The 2021 Global Payments Report, Worldpay from FIS, March 2021

7 https://source.android.com/security/bulletin

8 https://support.apple.com/en-us/HT201222

9 https://9to5mac.com/2020/08/01/new-unpatchable-exploit-allegedly-found-on-apples-secure-enclave-chip-heres-what-it-could-mean/

10 https://threatpost.com/mobile-adware-booms-attacks/164386/

11 https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data

12 https://latesthackingnews.com/2020/07/12/cerberus-malware-emerged-on-play-store-impersonating-cryptocurrency-converter-app/

13 https://thehackernews.com/2020/11/watch-out-new-android-banking-trojan.html

14 https://securityintelligence.com/posts/massive-fraud-operation-evil-mobile-emulator-farms/

15 https://owasp.org/www-project-mobile-top-10/

16 https://www.cvedetails.com/top-50-products.php?year=2021

17 Mobile Security Index 2020 Financial services spotlight, Verizon

18 https://www.first.org/cvss/

Commencez à protéger vos applications dès aujourd'hui.
Pour une analyse gratuite de votre application mobile, veuillez visiter :
https://www.zimperium.com/contact-us

ZIMPERIUM®

zimperium.com
844.601.6760 info zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244